IN THE CLAIMS:

Please amend the claims as follows.

1. (Currently Amended) Authentication method for a telecommunications network, ~~especially for an IF network,~~ the method including the steps of

transmitting from a terminal ~~(TE1)~~ to the network an authenticator and a data unit ~~(SPI)~~ containing information relating to ~~the~~ a manner in which the authenticator is formed, and

in the network, determining a check value by means of the data unit, wherein the check value ~~being~~ is compared with the said authenticator,

~~characterized by~~

using ~~such~~ an identification unit in the terminal of the network which receives a challenge as input from which it is possible to determine a response and a key essentially in the same way as in ~~the~~ a subscriber identification module of a known mobile communications system,

generating a set of subscriber-specific authentication data blocks into the network, each data block containing a challenge, a response and a key, whereby the generation is performed in the same manner as in the ~~said~~ mobile communications system,

transmitting at least some of the challenges contained in the authentication data blocks to the terminal,

choosing one of the challenges for use in the terminal, and based on ~~this~~ the challenge, determining a response and a key to be used with ~~the~~ an aid of the subscriber identity module of the terminal,

notifying the network with the aid of the ~~said~~ data unit of which key corresponding to which challenge was chosen, and

determining the authenticator and the ~~said~~ check value with the aid of the chosen key.

2. (Currently Amended) Method as defined in claim 1, ~~characterized in that~~ wherein the data unit is ~~the~~ a SPI (Security Parameter Index) in the registration message of the ~~Mobile~~ mobile IP protocol.

3. (Currently Amended) Method as defined in claim 1, ~~characterized in that~~ wherein the value of the response determined at the terminal is inserted into the data unit.

4. (Currently Amended) Method as defined in claim 1, ~~characterized in that~~ wherein the challenges are sorted in an order at the terminal with the aid of predetermined sorting criteria and a consecutive number corresponding to the chosen challenge is inserted into the data unit.

5. (Currently Amended) Method as defined in claim 1, ~~characterized in that~~ wherein the identification unit used in the terminal is the subscriber identity module ~~SIM~~

used by the known GSM system and the ~~said~~ authentication data blocks are authentication triplets used by the GSM system.

6. (Currently Amended) Method as defined in claim 5, ~~characterized in that~~ wherein the authentication triplets are fetched from the authentication centre ~~AuC~~ of the GSM system.

7. (Currently Amended) Method as defined in claim 6, ~~characterized in that~~ wherein the challenges to be transmitted to the terminal are transmitted by using a known short message switching service.

8. (Currently Amended) Method as defined in claim 1, ~~characterized in that~~ wherein the challenges to be transmitted to the terminal are transmitted in an IP datagram to be sent through an IP network.

9. (Currently Amended) Method as defined in claim 1 for an IP network, ~~characterized in that~~ wherein the authentication data blocks are transmitted to the home agent of the terminal and with the aid of the ~~said~~ data unit message is given to the home agent about which key corresponding to which challenge was chosen, whereby the ~~said~~ check value is determined in the home agent.

10. (Currently Amended) Authentication system for a telecommunications network, ~~especially for an IP network,~~ the system including

in a terminal ~~(TE1)~~ of the network, first message transmission means ~~(MEB)~~ for transmitting an authenticator and a data unit ~~(SPI)~~ to the network, the data unit including information relating to the manner in which the authenticator is formed, and

checking means ~~(HA)~~ for determining a check value with ~~the~~ aid of the data unit,

~~characterized in that~~ wherein

the terminal of the network includes such an identification unit, which receives as input a challenge from which a response and a key ~~can be~~ are defined essentially in ~~the~~ a same manner as in ~~the~~ a subscriber identity module of a known mobile communications system,

the system ~~contains~~ includes generating means ~~(HLR/AuC)~~ for generating authentication data blocks in the same manner as in the ~~said~~ mobile communications system, the authentication data blocks ~~being such that each of them contains~~ include a challenge, a response and a key,

the system includes transmission means for transmitting challenges contained by the authentication data blocks to the terminal, and

the terminal includes selection means ~~(SB)~~ for selecting one challenge for use,

the first message transmission means ~~(MEB)~~ insert such a value into the ~~said~~ data unit which indicates which key corresponding to which challenge was selected for use in the terminal, and

the first message transmission means ~~(MEB)~~ determine the authenticator and the checking means determine the ~~said~~ check value based on the selected key.

11. (Currently Amended) System as defined in claim 10, ~~characterized in that~~ wherein the identification unit located in connection with the terminal is a subscriber identity module ~~SIM~~ used in the ~~GSM~~ mobile communications system.

12. (Currently Amended) System as defined in claim 10, ~~characterized in that~~ wherein the said generating means include an authentication centre ~~AuC~~ of the ~~GSM~~ mobile communications system.

13. (Currently Amended) System as defined in claim 10, ~~characterized in that~~ wherein the said transmission means include means ~~(SMSC)~~ for carrying out a known short message switching service.

14. (New) An authentication method for a telecommunications network, said method comprising:

generating a set of subscriber-specific authentication data blocks, each authentication data block containing a challenge, a response and a key,

transmitting at least some of the challenges contained in the authentication data blocks to a terminal,

receiving an authenticator and a data unit containing information relating to a manner in which the authenticator is formed from the terminal,

determining based on said data unit which challenge was chosen by the terminal, and

determining a check value with the key corresponding to the chosen challenge, said check value to be compared with the authenticator.

15. (New) An authentication method as defined in claim 14, wherein said data unit is a security parameter index in the registration message of a Mobile IP protocol.

16. (New) An authentication method as defined in claim 14, wherein said data unit comprises the response corresponding to the chosen challenge.

17. (New) An authentication method for a terminal, said method comprising:

receiving a set of challenges from a telecommunications network,

choosing one challenge from the set of challenges,

determining a response and a key based on the chosen challenge,

determining an authenticator based on the key corresponding to the chosen challenge, and

transmitting said authenticator and a data unit to the telecommunications network, said data unit relating to the manner in which the authenticator is formed and

notifying the telecommunications network of the chosen challenge.

18. (New) An authentication method as defined in claim 17, wherein said data unit is a security parameter index in the registration message of a Mobile IP protocol.

19. (New) An authentication method as defined in claim 17, wherein said data unit comprises the response corresponding to the chosen challenge.

20. (New) A telecommunications network configured to

generate a set of subscriber-specific authentication data blocks, each authentication data block containing a challenge, a response and a key,

transmit at least some of the challenges contained in the authentication data blocks to a terminal,

receive an authenticator and a data unit containing information relating to a manner in which the authenticator is formed,

determine based on said data unit which challenge was chosen by the terminal,

determine a check value with the key corresponding to the chosen challenge, said check value to be compared with the authenticator.

21. (New) A terminal for a telecommunications network, said terminal configured to

receive a set of challenges from a telecommunications network,

choose one challenge from the set of challenges,

determine a response and a key based on the chosen challenge,

determine an authenticator based on the key corresponding to the chosen challenge, and

transmit said authenticator and a data unit to the telecommunications network, said data unit relating to the manner in which the authenticator is formed and notifying the telecommunications network of the chosen challenge.